14 CORREO SEGURO.

Hay aplicaciones de correo que permiten enviar y recibir correos cifrados y firmados digitalmente utilizando criptografía. Estas operaciones garantizan el intercambio seguro de información, proporcionando autenticación del emisor, integridad del mensaje, no repudio del origen, etc. En los siguientes apartados explicaremos detenidamente cómo tener correo seguro usando la tarjeta FNMT-RCM en los clientes de correo de **Microsoft** y de **Netscape**.

14.1 Correo seguro con Microsoft Outlook Express.

El intercambio seguro de información se basa en el uso de las claves públicas y privadas de usuarios. Las claves públicas son accesibles a todo el universo de usuarios y se envían junto con el certificado digital. En cambio las claves privadas son secretas y no pueden ser extraídas de la tarjeta.

Outlook Express utiliza CryptoAPI, con lo que para realizar operaciones criptográficas usará la librería **CeresCSP.dll**. Para utilizar todas las posibilidades del correo seguro entre dos usuarios es necesario que cada uno tenga el certificado del otro con sus claves públicas. La manera de obtenerlo es recibiendo un mensaje firmado, quedando así registrado en la libreta de direcciones.

14.1.1 Añadiendo un certificado a la cuenta.

Antes de poder enviar un correo firmado debemos indicarle a la aplicación de correo qué certificado queremos asociar a nuestra cuenta. Hemos comentado en apartados anteriores que era necesario que la dirección de correo electrónico asociada al certificado fuese la que quisiésemos utilizar como cuenta de correo habitual. Para asociar el certificado con nuestra cuenta de correo debemos ir al menú **Herramientas**, y allí seleccionar la opción **Cuentas**.

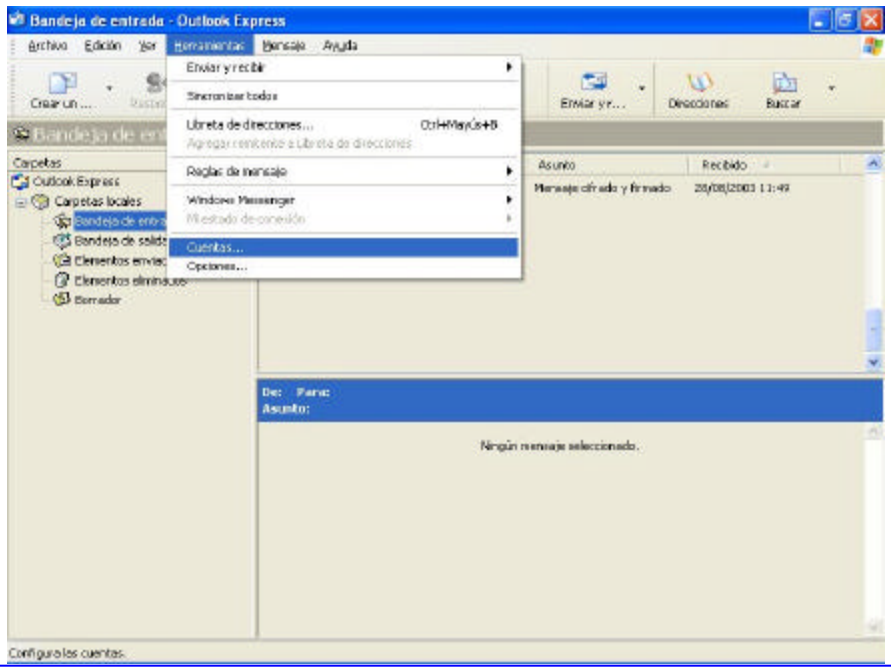

Figura 110: *Cuentas de correo en Outlook Express.*

Una vez seleccionada esa opción la aplicación de correo nos mostrará una ventana con las cuentas actuales del sistema. Ahí deberemos seleccionar nuestro servidor de correo y pulsar en el botón de Propiedades, desde donde pasaremos a configurar las opciones de seguridad.

Figura 111: *Cuentas de correo.*

Ya dentro de las propiedades de la cuenta, si seleccionamos la solapa de **Seguridad** vemos que aparecen dos cuadros vacíos con la etiqueta de **Certificado** que indican el certificado que se usará para las operaciones de firma y de cifrado digital.

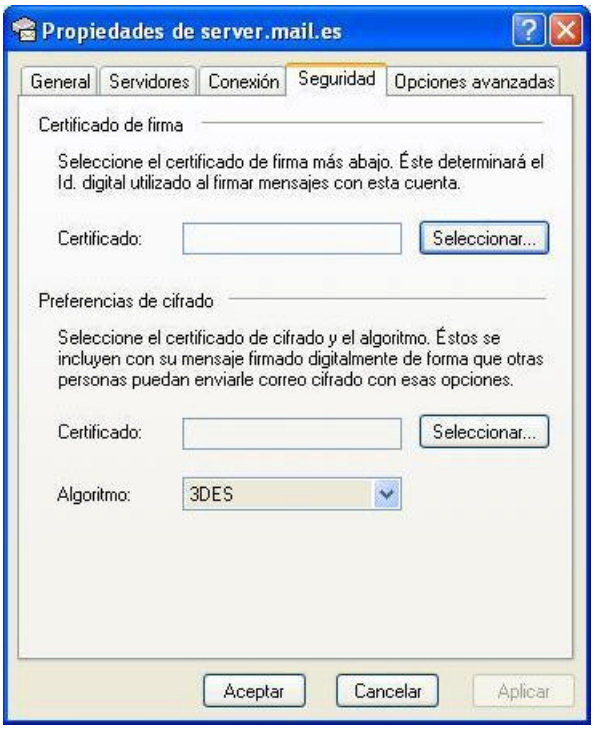

Figura 112: *Certificados actuales asociados a la cuenta de correo.*

Pulsando en los botones de **Seleccionar** pasaremos a la ventana de selección de certificados. Aquí se muestran los certificados instalados en el sistema y que tienen como dirección de correo asociada aquella que nosotros estamos utilizando. Puede que tengamos otros instalados y sin embargo no aparezcan en esta ventana. Será debido a que su dirección de correo es diferente.

Figura 113: *Certificados asociados a la cuenta actual de correo.*

Una vez tengamos seleccionado el certificado a utilizar, volveremos a la pantalla anterior y pulsaremos el botón de **Aplicar** para que los cambios tengan efecto. Ahora en los cuadros de texto que antes aparecían vacíos se mostrará el certificado que se va a usar en esa cuenta. Una vez asignada la identidad con la que vamos a realizar las operaciones criptográficas, podremos comenzar a enviar mensajes firmados digitalmente.

14.1.2 Firma y verificación de mensajes.

Para realizar una **firma** digital, el usuario utilizará su **clave privada** que se encuentra almacenada, junto con el resto de componentes del perfil criptográfico, en la tarjeta FNMT-RCM. Esa clave no puede ser extraída, por lo que no pueden existir copias de ella. Cuando queramos firmar un mensaje, la aplicación de correo nos solicitará la tarjeta cuyo número de serie coincida con el de aquella que contiene el certificado asociado a esa cuenta. Además, será necesario presentar el PIN de la tarjeta para acceder y utilizar la clave privada. De esta manera, si la tarjeta cayese en manos de otro individuo no podría realizar ninguna firma ya que no debería conocer su PIN.

Si queremos enviar un correo firmado a otro usuario, crearemos un nuevo mensaje de la forma habitual. Una vez que hayamos escrito el mensaje tenemos varias formas de indicar que queremos firmarlo. Podemos acceder al menú **Herramientas** y ahí seleccionar la opción **Firmar digitalmente**, o bien pulsar el botón **Firmar** de la barra de herramientas.
En la siguiente figura vemos un mensaje que va a ser firmado digitalmente utilizando el certificado que se seleccionó previamente para esa cuenta. En la imagen vemos que ha quedado pulsado el botón de **Firmar** y ha aparecido en la parte derecha un icono mostrando un pequeño sello rojo, indicando que el mensaje va a ser firmado antes de ser enviado. Cuando finalicemos el mensaje lo enviaremos normalmente y la aplicación de correo se realizará las operaciones de firma.

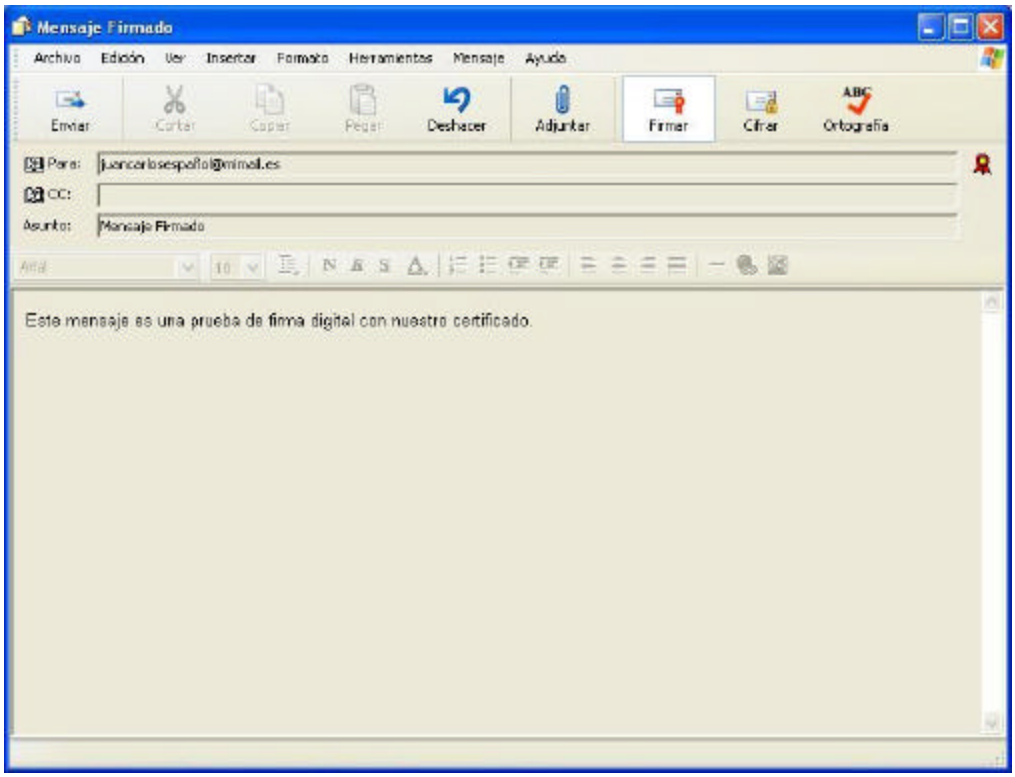

Figura 114: *Mensaje firmado listo para ser enviado.*

Como dijimos antes, para poder firmar digitalmente un mensaje es necesario usar nuestra clave privada, almacenada en la tarjeta, y presentar el PIN para tener acceso a ella. Por esto es imprescindible que la tarjeta que contiene el certificado se encuentre insertada en el lector. En caso de que no sea así aparecerá en pantalla una ventana solicitando la tarjeta correcta, cuyo **número de serie** debe coincidir con el indicado.

Inserte tarjeta
Por favor, inserte la tarjeta CERES "2109C4073710" en cualquier lector de tarjeta inteligente de su sistema.
Cancel

Figura 115: *Solicitud de la tarjeta correcta.*

Cuando la tarjeta esté disponible se solicitará su PIN. Será entonces cuando se realicen las operaciones de firma digital y se envíe el mensaje al destinatario, incluyendo el certificado del emisor.

En el cliente de correo del receptor aparecerá un nuevo mensaje con un icono que indica que dicho mensaje está firmado digitalmente. Al incluirse el certificado en el propio mensaje, cuando lo abramos se usará para verificar la firma e indicarnos si es correcta o no.

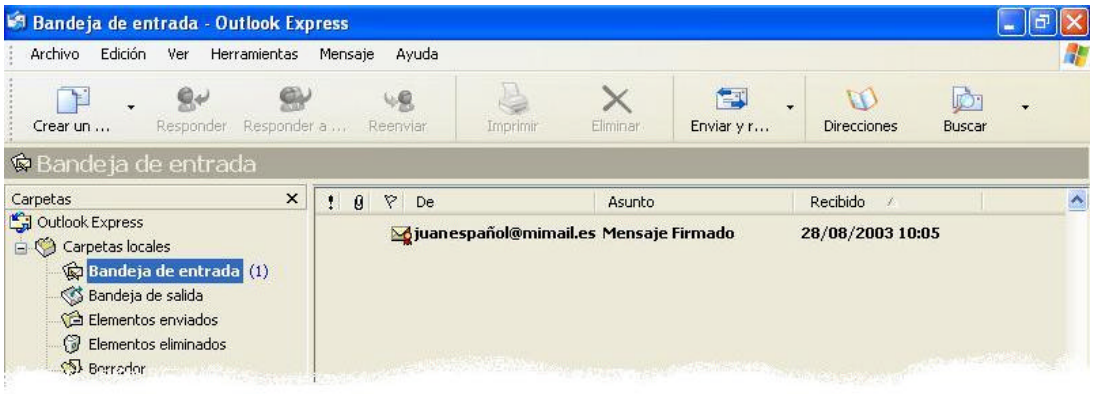
Bandeja de entrada - Outlook Express
Archivo Edición Ver Herramientas Mensaje Ayuda
Crear un ... Responder Responder a ... Reenviar Imprimir Eliminar Enviar y r... Direcciones Buscar
Bandeja de entrada
Carpetas
Outlook Express
Carpetas locales
Bandeja de entrada (1)
Bandeja de salida
Elementos enviados
Elementos eliminados
De Asunto Recibido
juanespañol@mimail.es Mensaje Firmado 28/08/2003 10:05

Figura 116: *Cliente de correo en el que se muestra el mensaje firmado.*

Si abrimos el mensaje firmado aparecerá una pantalla previa en la que *Outlook Express* nos indica que el mensaje ha sido firmado digitalmente. Tras pulsar el botón de "**Continuar"**, se usará el certificado para comprobar la autenticidad de la firma. Si puede verificar la firma recibida, el mensaje aparecerá normalmente. Si no, nos advertirá que no pudo ser verificada, aunque nos mostrará el texto del mensaje.

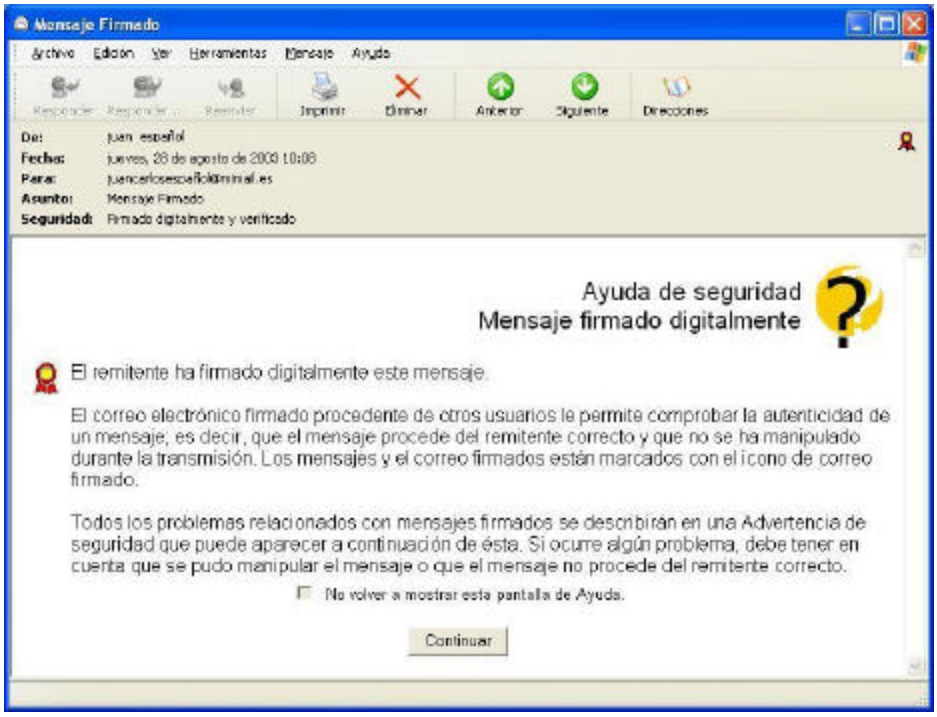
Mensaje Firmado
Archivo Edición Ver Herramientas Mensaje Ayuda
Imprimir
Eliminar
Anterior
Siguiente
Direcciones
De: juan español
Fecha: jueves, 28 de agosto de 2003 10:08
Para: juancarlosespañol@mimail.es
Asunto: Mensaje Firmado
Seguridad: Firmado digitalmente y verificado
Ayuda de seguridad
Mensaje firmado digitalmente
El remitente ha firmado digitalmente este mensaje.
El correo electrónico firmado procedente de otros usuarios le permite comprobar la autenticidad de un mensaje, es decir, que el mensaje procede del remitente correcto y que no se ha manipulado durante la transmisión. Los mensajes y el correo firmados están marcados con el icono de correo firmado.
Todos los problemas relacionados con mensajes firmados se describirán en una Advertencia de seguridad que puede aparecer a continuación de ésta. Si ocurre algún problema, debe tener en cuenta que se pudo manipular el mensaje o que el mensaje no procede del remitente correcto.
No volver a mostrar esta pantalla de Ayuda.
Continuar

Figura 117*: Aviso de correo FIRMADO.*

14.1.3 Cifrado y descifrado de mensajes.

Todo lo anterior era referente a la firma digital. Ahora comenzaremos con el **cifrado** y el **descifrado** de mensajes. Sabemos que para poder cifrar un mensaje debemos utilizar la clave pública del receptor. Esa clave pública se envía junto con el certificado, por lo que hasta que no lo tengamos no podremos enviarle un mensaje cifrado a ese usuario.

Una manera de obtener el certificado del receptor es recibir previamente un mensaje firmado por él y que lo incluya. De esta manera al añadirse a nuestra libreta de contactos, quedará reflejado el certificado asociado a ese usuario y que se usará para las operaciones criptográficas que lo requieran.

Cuando queramos cifrar un mensaje actuaremos normalmente, pero antes de enviarlo pulsaremos el botón de **Cifrar**, o bien lo indicaremos desde el menú de **Herramientas** del mensaje.

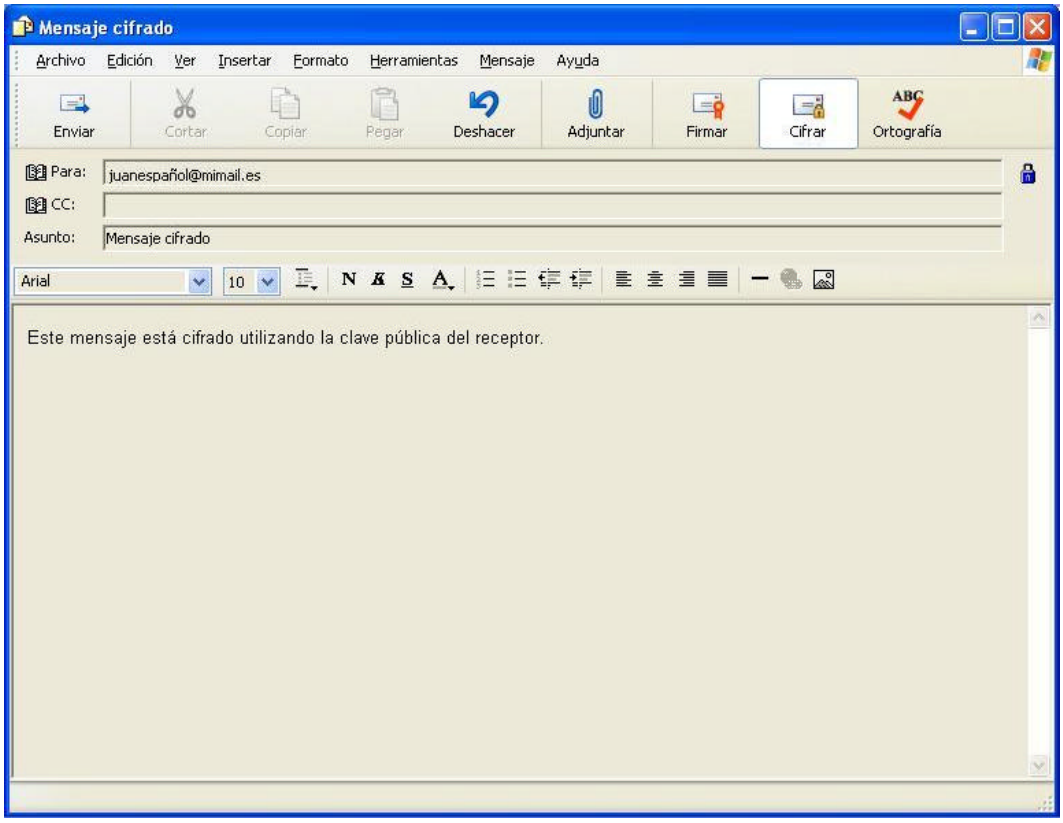

Figura 118: *Mensaje marcado para cifrar.*

En el mensaje aparecerá un pequeño icono de un *candado* en la parte derecha que indica que al enviar se va a realizar el cifrado del mensaje. Al contrario que con la firma

digital, ahora no es necesario tener insertada nuestra tarjeta inteligente ya que la clave que se va a usar es la del certificado del receptor.

Cuando el receptor del mensaje reciba el correo cifrado, le aparecerá marcado con el icono correspondiente.

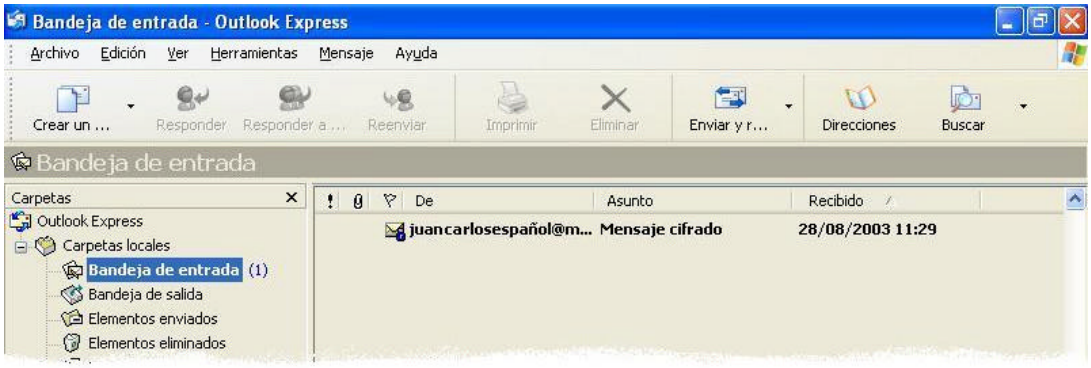
Bandeja de entrada - Outlook Express
Archivo Edición Ver Herramientas Mensaje Ayuda
Crear un ... Responder Responder a ... Reenviar Imprimir Eliminar Enviar y r... Direcciones Buscar
Bandeja de entrada
Carpetas
Outlook Express
Carpetas locales
Bandeja de entrada (1)
Bandeja de salida
Elementos enviados
Elementos eliminados
De Asunto Recibido
juancarlosespañol@m... Mensaje cifrado 28/08/2003 11:29

Figura 119: *Cliente de correo en el que se muestra el mensaje cifrado.*

Cuando se abra el mensaje nos aparecerá una advertencia indicándonos que ese mensaje está cifrado.

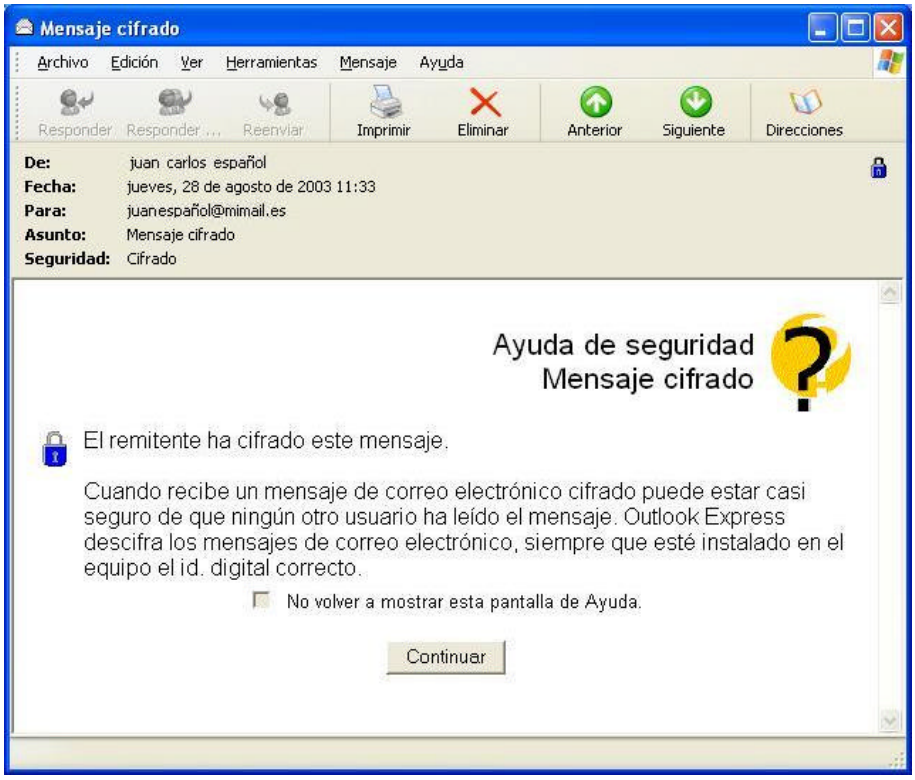
Mensaje cifrado
Archivo Edición Ver Herramientas Mensaje Ayuda
Responder Responder ... Reenviar Imprimir Eliminar Anterior Siguiente Direcciones
De: juan carlos español
Fecha: jueves, 28 de agosto de 2003 11:33
Para: juanespañol@mimail.es
Asunto: Mensaje cifrado
Seguridad: Cifrado
Ayuda de seguridad
Mensaje cifrado
El remitente ha cifrado este mensaje.
Cuando recibe un mensaje de correo electrónico cifrado puede estar casi seguro de que ningún otro usuario ha leído el mensaje. Outlook Express descifra los mensajes de correo electrónico, siempre que esté instalado en el equipo el id. digital correcto.
No volver a mostrar esta pantalla de Ayuda.
Continuar

Figura 120: *Aviso de correo CIFRADO.*

Para poder abrirlo necesitaremos nuestra tarjeta FNMT-RCM en la que se encuentra nuestra **clave privada**, necesaria para descifrar el mensaje. Si no estuviera insertada,

aparecería una ventana solicitando la tarjeta cuyo número de serie corresponda con la asociada al certificado.
Cuando queramos enviar un correo que esté a la vez **cifrado y firmado** realizaremos las mismas operaciones descritas anteriormente. Al realizarse una operación de firma digital y otra de cifrado, será necesario tener insertada la tarjeta con nuestra clave privada y además tener instalado el certificado del receptor del mensaje.

Antes de enviar el correo pulsaremos los botones de **Firmar** y **Cifrar**, mostrándose en este caso los iconos de las dos operaciones.

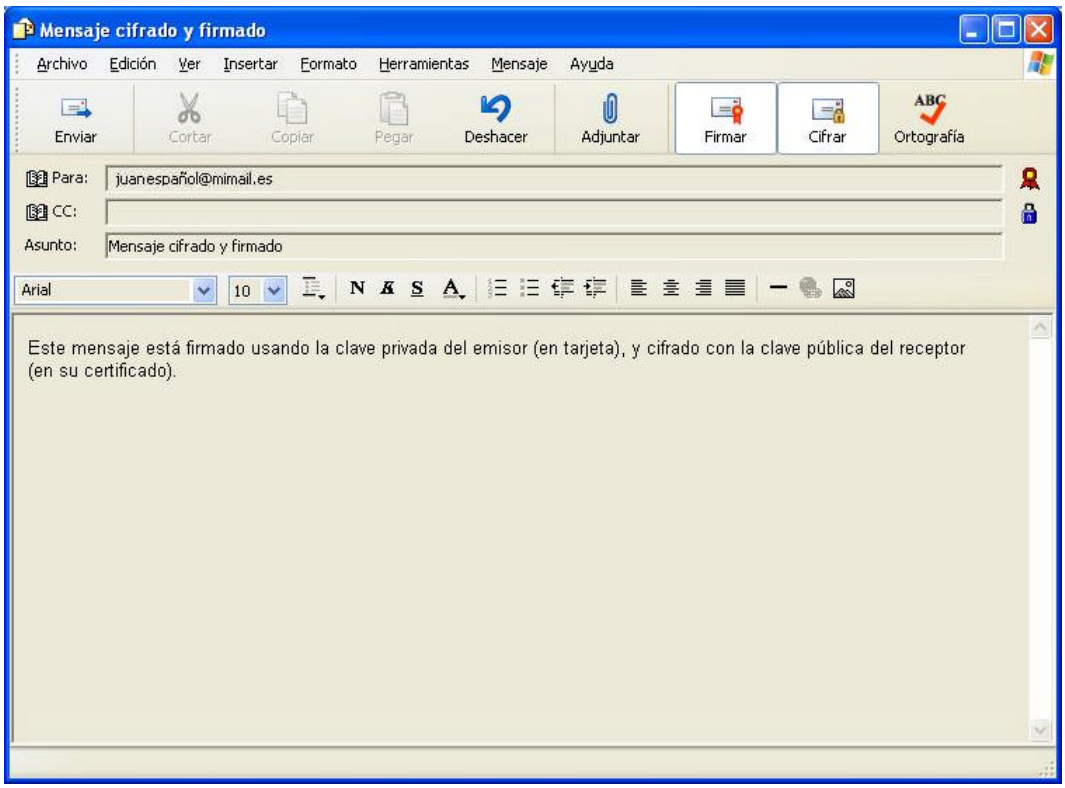

Figura 121*: Mensaje cifrado y firmado digitalmente.*

A continuación se intentará acceder a la tarjeta para firmar el mensaje. Si no estuviera insertada en el lector o la tarjeta actual no fuese la que está asociada al certificado instalado, aparecerá una ventana informándonos del error y solicitando aquella cuyo número de serie coincida con el indicado.

Inserte tarjeta
Por favor, inserte la tarjeta CERES "2109C4073710" en cualquier lector de tarjeta inteligente de su sistema.
Cancel

Figura 122: *Solicitud de tarjeta con número de serie determinado.*

Al recibir el mensaje veremos que el icono que aparece junto a él es solamente el de *cifrado*. Esto es debido a que el descifrado es la primera operación que se llevará a cabo, para después proceder con la verificación de la firma digital.

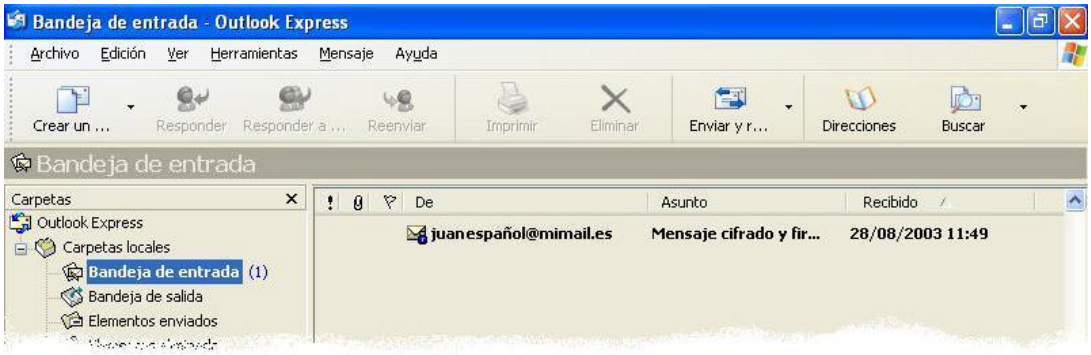
Bandeja de entrada - Outlook Express
Archivo Edición Ver Herramientas Mensaje Ayuda
Crear un ... Responder Responder a ... Reenviar Imprimir Eliminar Enviar y r... Direcciones Buscar
Bandeja de entrada
Carpetas
Outlook Express
Carpetas locales
Bandeja de entrada (1)
Bandeja de salida
Elementos enviados
De Asunto Recibido
juanespañol@mimail.es Mensaje cifrado y fir... 28/08/2003 11:49

Figura 123: *Cliente de correo con mensaje cifrado y firmado.*

A la hora de abrir un correo que esté cifrado y firmado, el mensaje que apareceré es similar a los anteriores, informándonos del estado del correo.

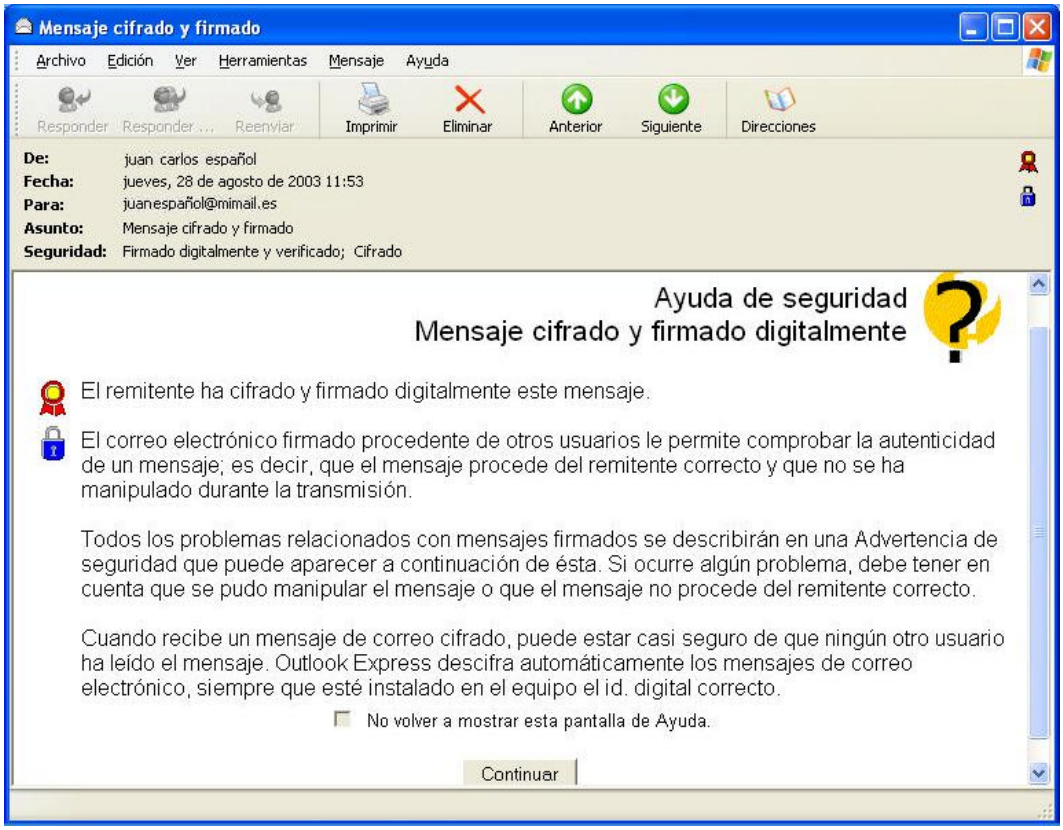
Mensaje cifrado y firmado
Archivo Edición Ver Herramientas Mensaje Ayuda
Responder Responder ... Reenviar Imprimir Eliminar Anterior Siguiente Direcciones
De: juan carlos español
Fecha: jueves, 28 de agosto de 2003 11:53
Para: juanespañol@mimail.es
Asunto: Mensaje cifrado y firmado
Seguridad: Firmado digitalmente y verificado; Cifrado
Ayuda de seguridad
Mensaje cifrado y firmado digitalmente
El remitente ha cifrado y firmado digitalmente este mensaje.
El correo electrónico firmado procedente de otros usuarios le permite comprobar la autenticidad de un mensaje; es decir, que el mensaje procede del remitente correcto y que no se ha manipulado durante la transmisión.
Todos los problemas relacionados con mensajes firmados se describirán en una Advertencia de seguridad que puede aparecer a continuación de ésta. Si ocurre algún problema, debe tener en cuenta que se pudo manipular el mensaje o que el mensaje no procede del remitente correcto.
Cuando recibe un mensaje de correo cifrado, puede estar casi seguro de que ningún otro usuario ha leído el mensaje. Outlook Express descifra automáticamente los mensajes de correo electrónico, siempre que esté instalado en el equipo el id. digital correcto.
No volver a mostrar esta pantalla de Ayuda.
Continuar

Figura 124: *Aviso de correo CIFRADO y FIRMADO.*

Para abrirlo necesitaremos nuestra tarjeta FNMT-RCM con nuestro certificado almacenado para descifrar el mensaje, además del certificado del emisor para poder verificar su firma digital.

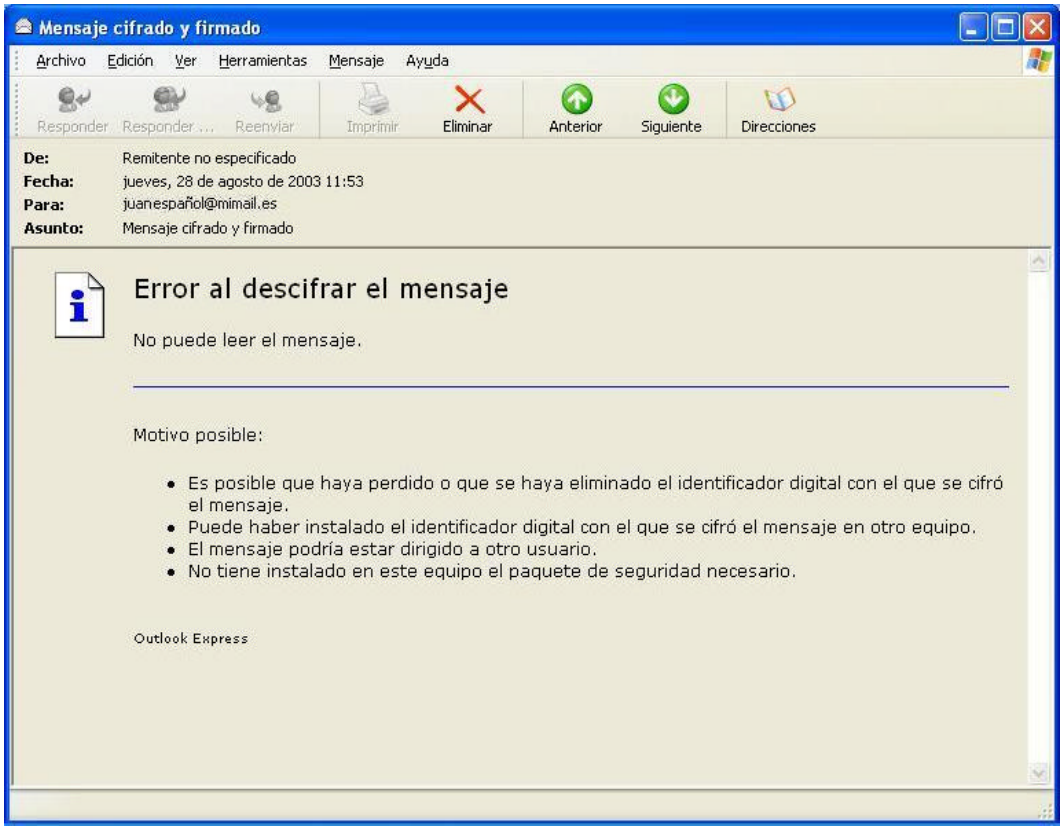
Mensaje cifrado y firmado
Archivo Edición Ver Herramientas Mensaje Ayuda
Responder Responder ... Reenviar Imprimir Eliminar Anterior Siguiente Direcciones
De: Remitente no especificado
Fecha: jueves, 28 de agosto de 2003 11:53
Para: juanespañol@mimail.es
Asunto: Mensaje cifrado y firmado
Error al descifrar el mensaje
No puede leer el mensaje.
Motivo posible:
Es posible que haya perdido o que se haya eliminado el identificador digital con el que se cifró el mensaje.
Puede haber instalado el identificador digital con el que se cifró el mensaje en otro equipo.
El mensaje podría estar dirigido a otro usuario.
No tiene instalado en este equipo el paquete de seguridad necesario.
Outlook Express

Figura 125*: Error al descifrar el mensaje.*

14.2 Correo seguro con Netscape Messenger.

El cliente de correo **Netscape Messenger** también nos permite utilizar correo seguro entre usuarios, soportando tareas de cifrado, firma digital, verificación, etc. Seguramente la mayor diferencia que existe entre este cliente de correo y el de Microsoft es en la librería sobre la que basan dichas operaciones para realizarlas sobre dispositivos tales como tarjetas inteligentes. Mientras Outlook utiliza **CryptoAPI**, Messenger usa **PKCS#11**. Esto no implica que sean incompatibles, ni mucho menos, ambos sistemas. El correo cifrado y/o firmado con uno de ellos podrá ser descifrado y/o verificado con cualquiera de los dos sistemas.

Hemos indicado en apartados anteriores que la librería PKCS#11 de la FNMT-RCM es **pkcsv2gk.dll**. Esta librería deberá estar convenientemente instalada como módulo criptográfico en el sistema para que nos dé acceso a la tarjeta FNMT-RCM (para su instalación, ver apartado de *Netscape* dentro del *Gestor de aplicaciones*).

14.2.1 Añadiendo un certificado a la cuenta.

Con la librería PKCS#11 instalada (ver apartado **10.1.2**) deberemos configurar las opciones del *Messenger* para que asocie a nuestra cuenta el certificado digital que nosotros queramos utilizar. Al igual que ocurría con Outlook Express, es necesario que la dirección de e-mail contenida en el certificado se corresponda con aquella que vamos a usar ahora.

Para configurar estas opciones deberemos pulsar el botón de '**Security**" que aparece en el propio mensaje o desde el navegador Netscape Navigator.

Figura 126: *Configuración de seguridad desde la ventana de mensajes.*

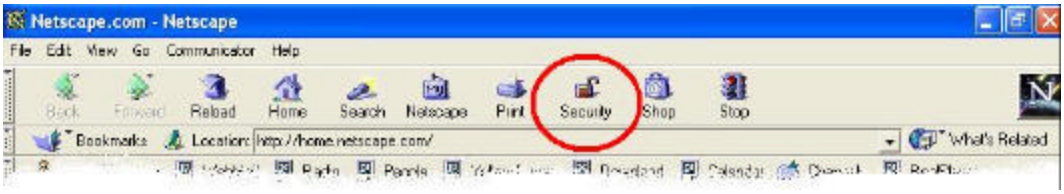
Netscape.com - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://home.netscape.com/
What's Related

Figura 127: *Configuración de seguridad desde Netscape Navigator.*

En esa pantalla, dentro de **Messenger**, seleccionaremos las opciones de envío y el certificado que queremos usar con nuestra cuenta.

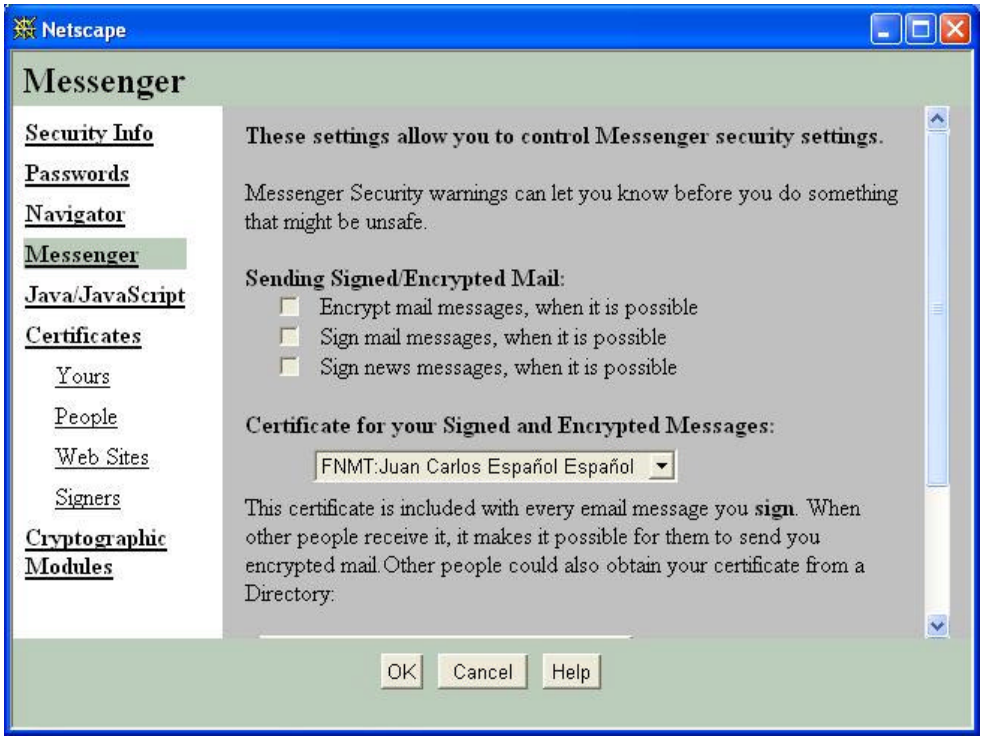
Netscape
Messenger
Security Info
Passwords
Navigator
Messenger
Java/JavaScript
Certificates
Yours
People
Web Sites
Signers
Cryptographic Modules
These settings allow you to control Messenger security settings.
Messenger Security warnings can let you know before you do something that might be unsafe.
Sending Signed/Encrypted Mail:
Encrypt mail messages, when it is possible
Sign mail messages, when it is possible
Sign news messages, when it is possible
Certificate for your Signed and Encrypted Messages:
FNMT:Juan Carlos Español Español
This certificate is included with every email message you sign. When other people receive it, it makes it possible for them to send you encrypted mail. Other people could also obtain your certificate from a Directory:
OK
Cancel
Help

Figura 128: *Selección del certificado a usar.*

14.2.2 Firma y verificación de mensajes.

En cuanto al interfaz de Netscape Messenger es similar al de Microsoft Outlook Express, y la forma de operar será también muy parecida.

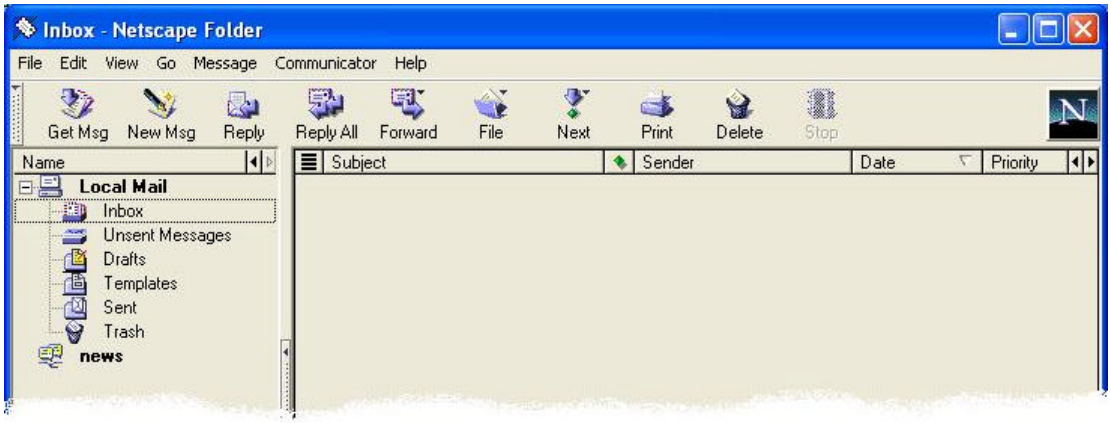

Figura 129: *Interfaz de Netscape Communicator.*

Cuando escribamos un mensaje que queramos que sea **firmado**, deberemos seleccionar la solapa de "**Opciones de envío de mensajes**", situada en la parte izquierda de la pantalla. Entonces aparecerán una serie de opciones de envío, donde podremos indicar si queremos cifrar, firmar digitalmente, etc.

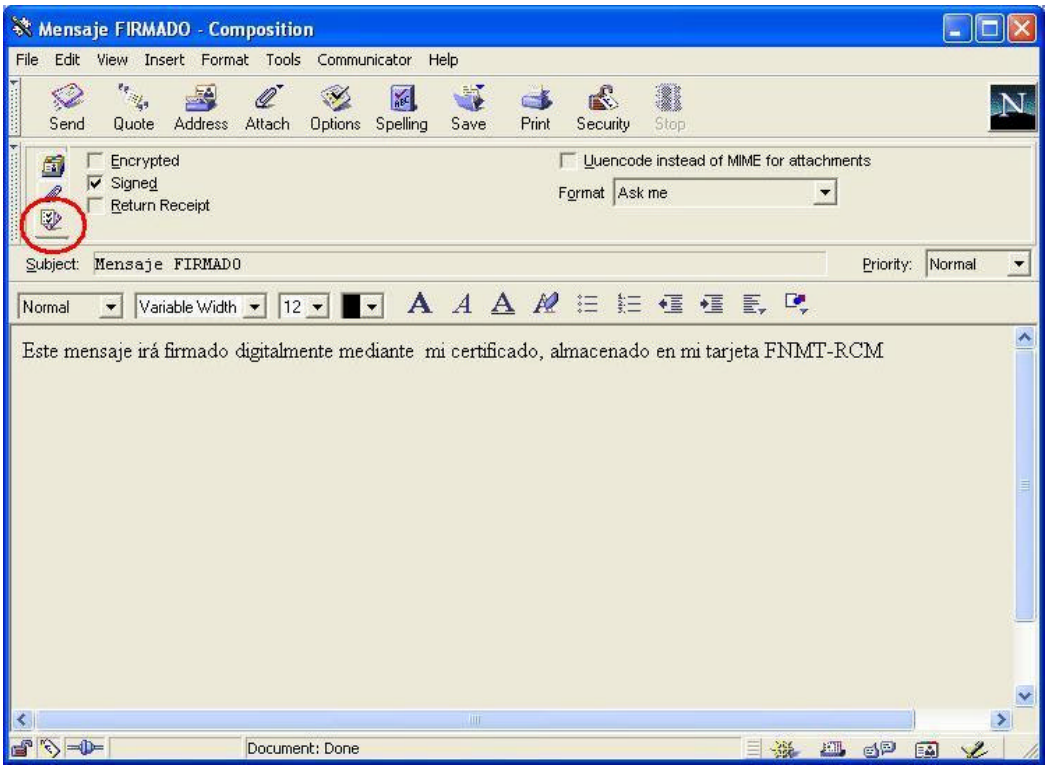
Mensaje FIRMADO - Composition
File Edit View Insert Format Tools Communicator Help
Send Quote Address Attach Options Spelling Save Print Security Stop
Encrypted
Signed
Return Receipt
Uuencode instead of MIME for attachments
Format Ask me
Subject: Mensaje FIRMADO
Priority: Normal
Normal Variable Width 12
Este mensaje irá firmado digitalmente mediante mi certificado, almacenado en mi tarjeta FNMT-RCM
Document: Done

Figura 130: *Opciones de envío para correo seguro.*

Si ya tenemos configurado el sistema para que utilice un certificado en tarjeta FNMT-RCM, cuando enviemos el mensaje la aplicación nos pedirá que introduzcamos el PIN de la tarjeta. Al contrario de lo que sucedía con Outlook Express, en Messenger sólo nos pedirá el PIN una vez, quedando validadas las operaciones posteriores con tarjeta hasta que se cierre la aplicación o hasta que se extraiga la tarjeta del lector.

Figura 131: *Ventana de solicitud del PIN de la tarjeta.*

En caso de no introducir correctamente el PIN o no tener acceso a la tarjeta, Netscape Messenger nos mostrará un mensaje de error en el que nos informará de que no ha sido posible enviar el mensaje firmado. Esto, como sabemos, es debido a que al no habernos autenticado en la tarjeta no podemos acceder al uso de sus claves.

Netscape
This message cannot be encrypted or signed because you do not yet have an email certificate. Click on the `Security' icon for more information about certificates.
Aceptar

Figura 132: *Información sobre seguridad del mensaje.*

Cuando recibamos un mensaje firmado y lo abramos, el cliente de correo nos informará si ese mensaje está cifrado, firmado o ambas cosas a la vez. Podemos verlo rápidamente observando los iconos que aparecerán en la parte derecha del correo.

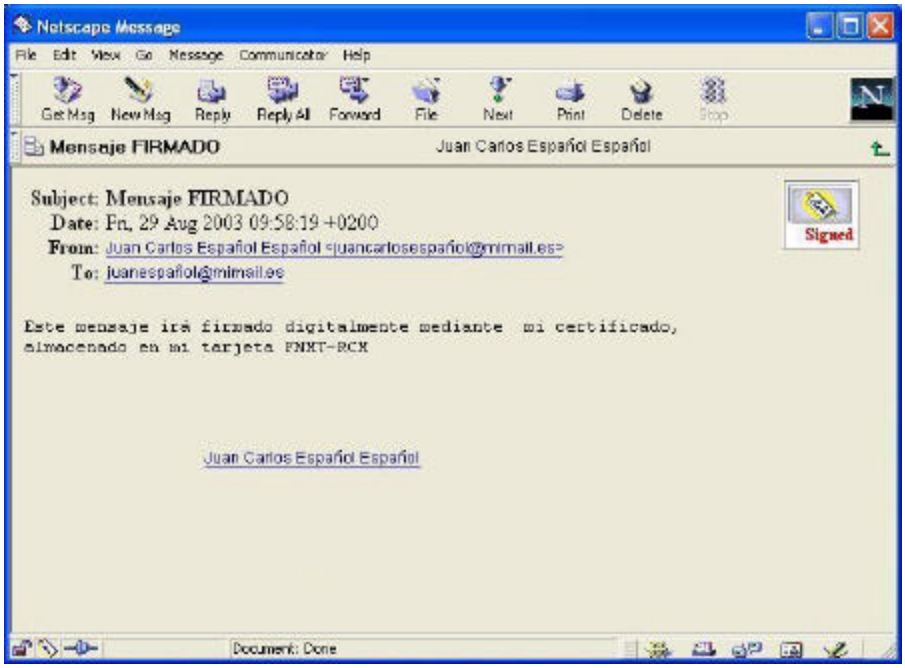
Netscape Message
File Edit View Go Message Communicator Help
Get Msg New Msg Reply Reply All Forward File Next Print Delete Stop
Mensaje FIRMADO
Juan Carlos Español Español
Subject: Mensaje FIRMADO
Date: Fri, 29 Aug 2003 09:58:19 +0200
From: Juan Carlos Español Español <juancarlosespañol@mimail.es>
To: juanespañol@mimail.es
Signed
Este mensaje irá firmado digitalmente mediante mi certificado, almacenado en mi tarjeta FNMT-RCM
Juan Carlos Español Español
Document: Done

Figura 133: *Información sobre seguridad del mensaje.*

En la figura anterior podemos observar el icono que indica que el mensaje está firmado (**Signed**). En caso de que también estuviese cifrado (**Encrypted**), aparecería otro icono similar junto a él, avisándonos de ello.

Esos iconos nos darán acceso a la pantalla de seguridad, en la que nos informará si la firma ha podido ser verificada, el formato de cifrado que se utilizó, etc.

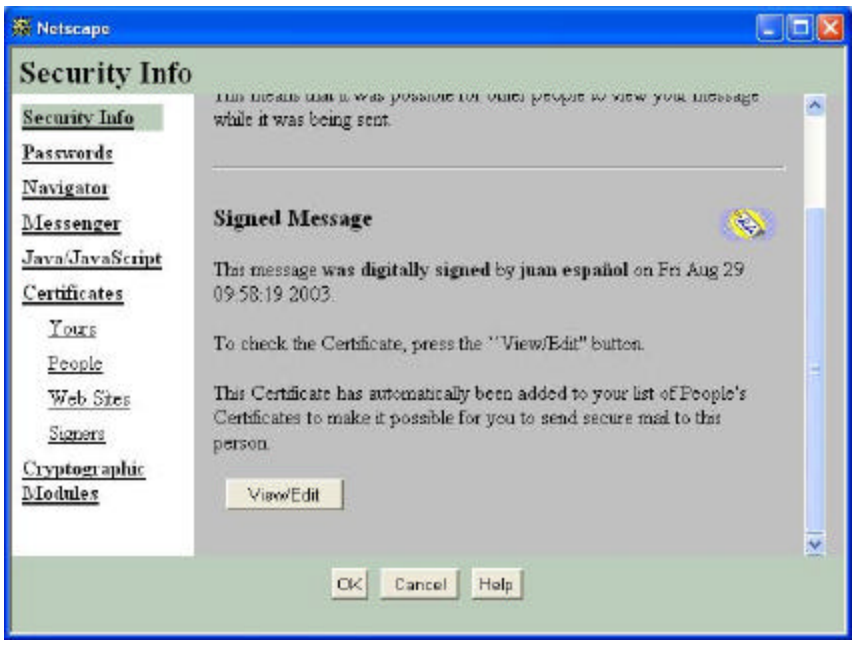

Figura 134: *Información sobre seguridad del mensaje.*

14.2.3 Cifrado y descifrado de mensajes.

Para los mensajes **cifrados** deberemos seguir el mismo procedimiento. Desde la ventana de creación del nuevo mensaje, en las opciones de envío marcaremos **Cifrado** (**Encrypted**).

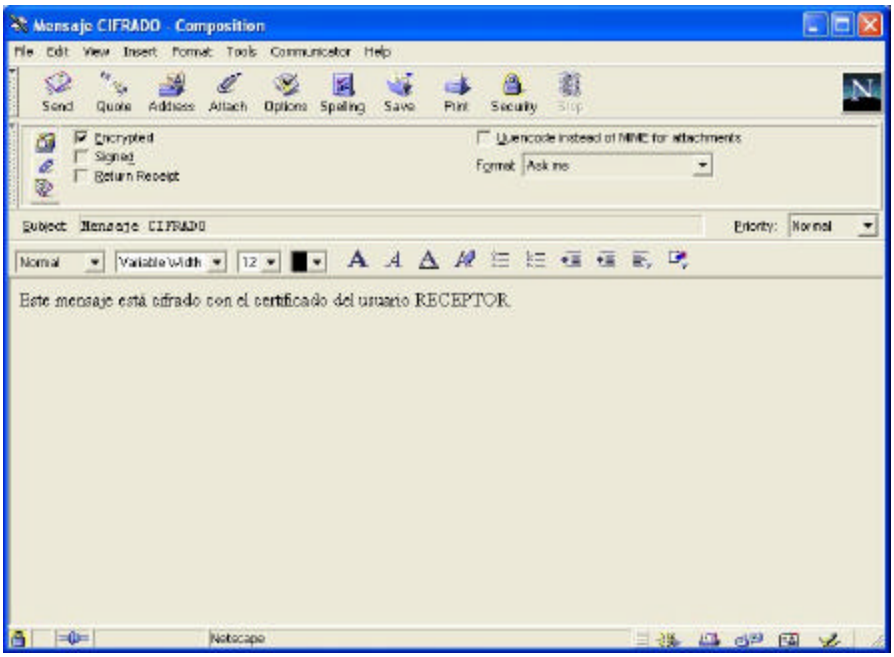

Figura 135: *Mensaje cifrado.*

Al abrir el mensaje comprobaremos que aparece el icono informándonos de que había sido cifrado y que nos permite acceder a la información sobre él.

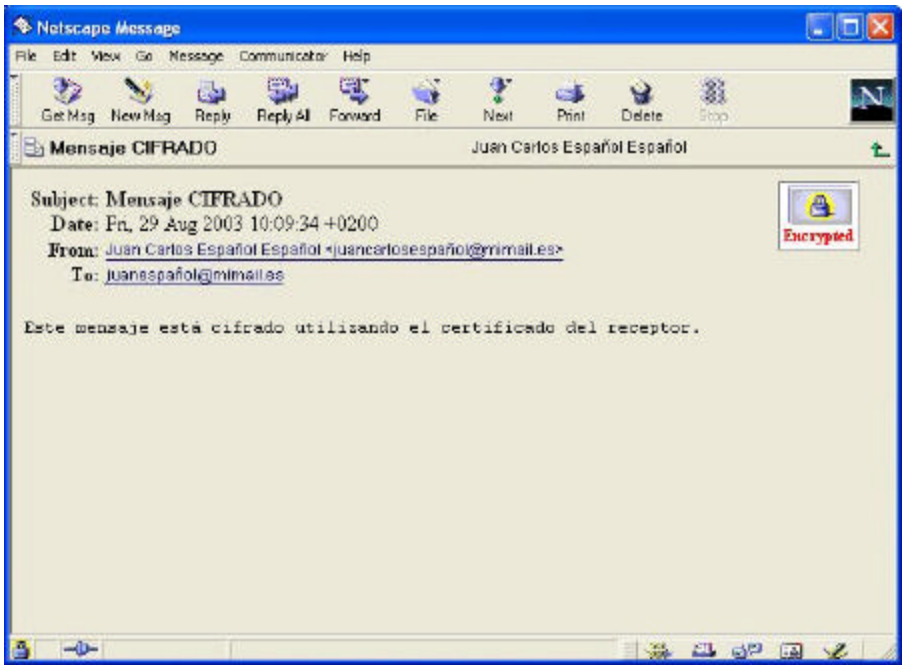

Figura 136: *Mensaje cifrado recibido por el cliente de correo.*

Al igual que ocurría con los correos firmados, si pulsamos el icono de cifrado, aparecerá la ventana de seguridad, explicándonos la operación de cifrado del mensaje.

Figura 137: *Información sobre seguridad del mensaje.*

Una vez comentadas cómo serían las operaciones de firma y de cifrado, sólo queda indicar que también es posible realizar ambas cosas sobre un mismo correo. Bastará con indicarlo en las opciones de envío.

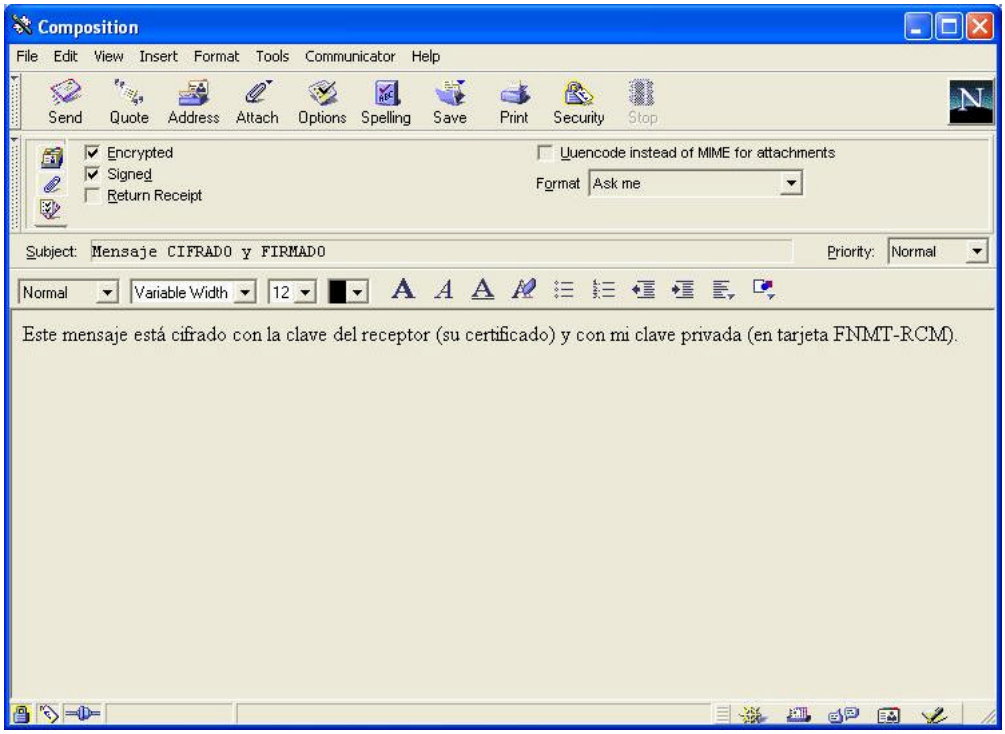
Composition
File Edit View Insert Format Tools Communicator Help
Send Quote Address Attach Options Spelling Save Print Security Stop
Encrypted
Signed
Return Receipt
Uuencode instead of MIME for attachments
Format Ask me
Subject: Mensaje CIFRADO y FIRMADO
Priority: Normal
Normal Variable Width 12
Este mensaje está cifrado con la clave del receptor (su certificado) y con mi clave privada (en tarjeta FNMT-RCM).

Figura 138: *Mensaje cifrado y firmado.*

Al recibir un mensaje cifrado y firmado digitalmente, la pantalla que se nos muestra será similar a la que aparece a continuación.

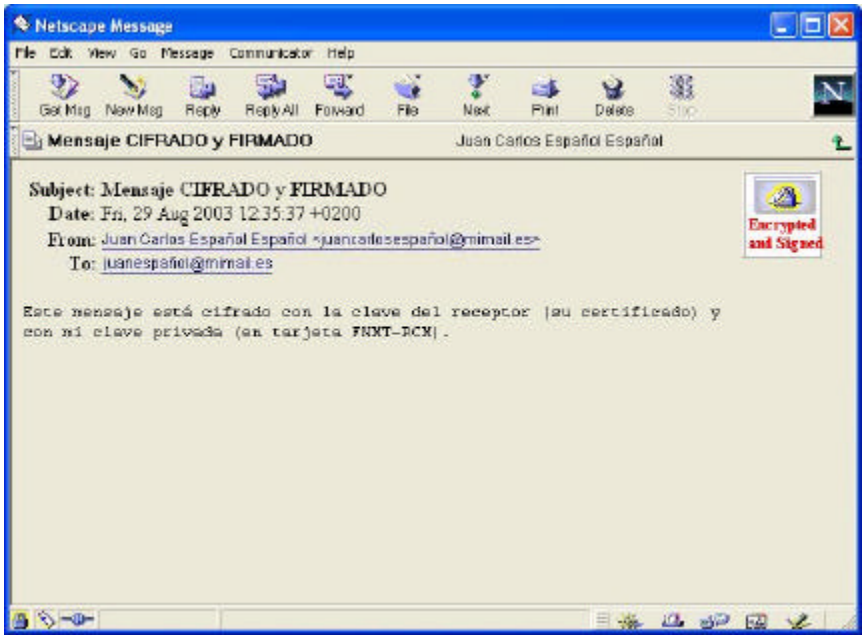
Netscape Message
File Edit View Go Message Communicator Help
Get Msg New Msg Reply Reply All Forward File Next Print Delete Stop
Mensaje CIFRADO y FIRMADO
Juan Carlos Español Español
Subject: Mensaje CIFRADO y FIRMADO
Date: Fri, 29 Aug 2003 12:35:37 +0200
From: Juan Carlos Español Español <juancarlosespañol@mimail.es>
To: juanespañol@mimail.es
Encrypted and Signed
Este mensaje está cifrado con la clave del receptor (su certificado) y con mi clave privada (en tarjeta FNMT-RCM).

Figura 139: *Información sobre seguridad del mensaje.*

Si pulsamos sobre el icono de información de seguridad, aparecerá de nuevo la ventana de información correspondiente al mensaje recibido.

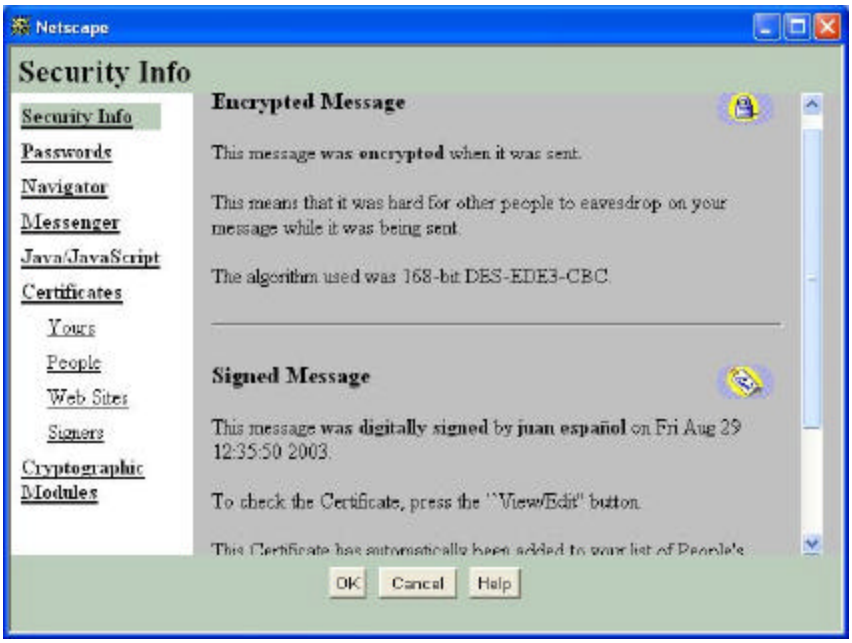

Figura 140: *Información sobre seguridad del mensaje.*

Capítulo 15

Conexión segura

15 CONEXIÓN SEGURA.

Otra de las funcionalidades que presentan las librerías **CeresCsp.dll** y **pkcsv2gk.dll** es que permiten la comunicación segura entre cliente-servidor. Para ello se utilizan protocolos de comunicación, tales como SSL, que permiten establecer un canal de comunicación seguro entre equipos.

En los siguientes apartados vamos a explicar brevemente la forma de conexión en los distintos navegadores.

15.1 Conexión segura en Microsoft Internet Explorer.

A lo largo de todo el documento hemos visto que para que un certificado almacenado en la tarjeta FNMT-RCM sea accesible a las aplicaciones de Microsoft, debe estar también instalado en el sistema.

Cuando una aplicación Web requiera una conexión segura, pasará el control al navegador, quien nos mostrará la ventana de certificados instalados, donde podremos seleccionar aquel con el que queremos conectarnos.

Figura 141: *Selección del certificado a utilizar.*